Comments on "Best conventional solutions to the King's problem"

Gen Kimura,[*] Hajime Tanaka,[†] and Masanao Ozawa[‡]

Graduate School of Information Sciences, Tohoku University, Aoba-ku, Sendai 980-8579, Japan
(Dated: February 1, 2008)

Conventional solutions to the (Mean) King's problem without using entanglement have been investigated by Aravind [P. K. Aravind, "Best conventional solutions to the King's problem", Z. Naturforsch. **58a**, 682 (2003)]. We report that the upper bound for the success probability claimed there is not valid in general, and give a condition for the claim to be justified.

The (Mean) King's problem [1, 2, 3] is a kind of quantum estimation problem with delayed (classical) information and has been studied in detail [2, 3], relating with an unsolved problem on the existence of a maximal set of mutually unbiased bases (MUBs) [4]. The standard approach to solve the King's problem is to utilize entanglement, and nowadays it is shown that the success probability is in fact 1 for any d level system [3]. On the other hand, Aravind [5] has considered the King's problem without using entanglement, in order to elucidate the role of entanglement in this problem. In this case he claimed the following upper bound of the success probability $P(d)$ for any d level system:

$$P(d) \leq \frac{2\sqrt{d} + d - 1}{\sqrt{d}(d+1)}.$$

For small d, this gives

d	2	3	4	5	8	9
$P(d)$	0.9024	0.7887	0.7000	0.6315	0.4972	0.4667

The purpose of this letter is, however, to show that this upper bound is not justified for $d \geq 3$ in general. We also give a condition for the claim to be justified.

We begin by recalling the setting of the King's problem without entanglement, as formulated in [5] by the following steps (A)-(E)F

(A) A physicist, Alice, prepares a d-level quantum system S in a state of her choosing and gives it to the king.

(B) The king carries out a projective measurement with respect to one of $d + 1$ MUBs $\{|\Psi_j^\mu\rangle\}_{j=1}^d$ ($\mu = 0, \ldots, d$) [6], and notes the output he obtained.

(C) The physicist carries out a control measurement in an orthonormal basis $\chi = \{|\chi_k\rangle\}_{k=1}^d$ on the system S.

(D) The king reveals which of the MUBs he has measured. (Delayed classical information.)

*Electronic address: gen@ims.is.tohoku.ac.jp
†Electronic address: htanaka@ims.is.tohoku.ac.jp
‡Electronic address: ozawa@math.is.tohoku.ac.jp

(E) The physicist is required to correctly predict the output of the king's measurement in Step (B). Let the physicist prepare a density operator ρ of the system S in Step (A). In Step (B), the king is supposed to randomly choose one of $d + 1$ MUBs. In other words, the probability that the king chooses the μth MUB is $\frac{1}{d+1}$. (Therefore, what we consider is a Bayes estimation problem with a uniform prior distribution.) It is assumed that the king's measurement is a projective measurement with respect to one of given $d + 1$ MUBs, so that the post measurement state in Step (B) is $|\Psi_j^\mu\rangle$ if the king chose the μth MUB and obtained his output j. In Step (C), the physicist is allowed to make measurements only on the system itself (the "conventional" solution [5]) which are described by an orthonormal basis $\chi = \{|\chi_k\rangle\}_{k=1}^d$ (namely a measurement of a nondegenerate observable) [7]. The conditional probability to obtain an output k given μ, j and a basis measurement χ is given by $P(k|\mu, j, \chi) = |\langle\Psi_j^\mu|\chi_k\rangle|^2$. Finally, in Step (E) the physicist is required to prepare a decision function $s : (k, \mu) \mapsto s_{k\mu} \in \{1, \ldots, d\}$ by which she guesses the king's output j based on her output k obtained in Step (C) and the post information μ revealed in Step (D). (Namely, she predicts the king's output to be $s_{k\mu}$ if she obtained the pair (k, μ) of her output k and the king's MUB μ.) Based on this setting, the physicist's strategy is to find a suitable input state ρ, a basis measurement χ, and a decision function s which maximize her success probability $P_d(\rho, \chi, s)$ to correctly predict King's output, where it is determined as $P_d(\rho, \chi, s) = \sum_{\mu=0}^d \frac{1}{d+1} P(\rho, \chi, s, \mu)$ with the conditional success probability $P(\rho, \chi, s, \mu)$ given by $P(\rho, \chi, s, \mu) = \sum_{j=1}^d P(j|\rho, \mu) \sum_{k=1}^d \delta_{j,s_{k\mu}} P(k|\mu, j, \chi)$. Thus the success probability $P_d(\rho, \chi, s)$ with respect to the physicist's choice (ρ, χ, s) for a d level system is given by

$$P_d(\rho, \chi, s)$$
$$= \frac{1}{d+1} \sum_{\mu=0}^d \sum_{k=1}^d \langle\Psi_{s_{k\mu}}^\mu|\rho|\Psi_{s_{k\mu}}^\mu\rangle |\langle\Psi_{s_{k\mu}}^\mu|\chi_k\rangle|^2. \quad (1)$$

Here we have two remarks on $P_d(\rho, \chi, s)$. First, since

it is an affine function (and hence a convex function) with respect to the input state ρ, its maximum is attained by a pure state. Second, with fixed ρ and χ, the optimal decision function $s_{\max}$ is given by

$$s_{\max}(k,\mu) \equiv \operatorname*{argmax}_{j=1,\ldots,d} \left[\langle \Psi_j^\mu | \rho | \Psi_j^\mu \rangle | \langle \Psi_j^\mu | \chi_k \rangle |^2 \right]. \quad (2)$$

(Here $\operatorname{argmax}_{j=1,\ldots,d}[F(j)]$ assigns a value j which maximizes the real function F on $\{1,\ldots,d\}$.) Indeed, from (1) it is easy to see $P_d(\rho,\chi,s) \leq P_d(\rho,\chi,s_{\max})$ for any decision function s.

Aravind claimed an upper bound of the success probability (1):

Claim 1 (Aravind [5]). *For any density operator ρ, a basis measurement with respect to an orthonormal basis $\chi = \{|\chi_k\rangle\}_{k=1}^d$, and a decision function $s : (k,\mu) \mapsto s_{k\mu} \in \{1,\ldots,d\}$, the success probability (1) on the guess of the king's output is bounded from above by*

$$P_d(\rho,\chi,s) \leq P_d(|\Psi_j^\mu\rangle\langle\Psi_j^\mu|,\chi,s) \leq \frac{2\sqrt{d}+d-1}{\sqrt{d}(d+1)}, \quad (3)$$

where $j \in \{1,\ldots,d\}$ and $\mu \in \{0,\ldots,d\}$.

Claim 1 includes two statements: (i) *An optimal input state can be taken from one of the basis vectors $|\Psi_j^\mu\rangle$ of the MUBs* (the first inequality in (3)); and (ii) it is bounded from above by $\frac{2\sqrt{d}+d-1}{\sqrt{d}(d+1)}$ (the second inequality in (3)).

Indeed (3) is true when $d = 2$, and one can also find a suitable choice of (ρ,χ,μ) to attain the bound [8]. However, as we shall see some counter examples, it is not justified for $d \geq 3$ in general.

Counter Example 1 (Case $d = 3$). Let $\{|\Psi_j^\mu\rangle\}_{j=1}^3$ ($\mu = 0,\ldots,3$) denote the MUBs constructed by Ivanović [9]. Let $\rho = |\varphi\rangle\langle\varphi|$ where

$$|\varphi\rangle = (0, \frac{i}{\sqrt{2}}, \frac{3+\sqrt{3}i}{2\sqrt{6}})^T, \quad (4)$$

and let $\chi = \{|\chi_k\rangle\}_{k=1}^3$ be the orthonormal basis defined by

$$|\chi_1\rangle = (\frac{1}{\sqrt{2}}, \frac{\sqrt{3}i}{2\sqrt{2}}, -\frac{\exp(\frac{3i\pi}{4})}{2\sqrt{2}})^T,$$

$$|\chi_2\rangle = (\frac{i}{\sqrt{2}}, \frac{\sqrt{3}}{2\sqrt{2}}, -\frac{\exp(\frac{i\pi}{4})}{2\sqrt{2}})^T,$$

$$|\chi_2\rangle = (0, \frac{\exp(\frac{-i\pi}{4})}{2}, \frac{\sqrt{3}}{2})^T.$$

Then, the success probability $P_3(\rho,\chi,s_{\max})$ with the optimal guess function (2) is given by

$$P_3(\rho,\chi,s_{\max}) = \frac{21+2\sqrt{2}+6\sqrt{6}}{32} \simeq 0.8212. \quad (5)$$

This is strictly greater than Aravind's bound $\frac{3+\sqrt{3}}{6} \simeq 0.7887$ for $d = 3$.

Aravind [5] also showed that the bound (3) is attainable for $d = 4$. To see that, he used the following MUBs:

$|\Psi_1^0\rangle = 1000$	$|\Psi_2^0\rangle = 0100$	$|\Psi_3^0\rangle = 0010$	$|\Psi_4^0\rangle = 0001$
$|\Psi_1^1\rangle = 1111$	$|\Psi_2^1\rangle = 1\bar{1}1\bar{1}$	$|\Psi_3^1\rangle = 11\bar{1}\bar{1}$	$|\Psi_4^1\rangle = 1\bar{1}\bar{1}1$
$|\Psi_1^2\rangle = 1ii\bar{1}$	$|\Psi_2^2\rangle = 1\bar{i}i1$	$|\Psi_3^2\rangle = 1\bar{i}i1$	$|\Psi_4^2\rangle = 1\bar{i}\bar{i}\bar{1}$
$|\Psi_1^3\rangle = 1\bar{1}ii$	$|\Psi_2^3\rangle = 11\bar{i}i$	$|\Psi_3^3\rangle = 11i\bar{i}$	$|\Psi_4^3\rangle = 1\bar{1}\bar{i}i$
$|\Psi_1^4\rangle = 1i\bar{1}i$	$|\Psi_2^4\rangle = 1\bar{i}1i$	$|\Psi_3^4\rangle = 1i1\bar{i}$	$|\Psi_4^4\rangle = 1\bar{i}1\bar{i}$

(The shorthand notation $|\Psi_j^\mu\rangle = abcd$ indicates that $|\Psi_j^\mu\rangle$ has the (unnormalized) form $(a,b,c,d)^T \in \mathbb{C}^4$, and $\bar{a}$ stands for the negative of a.) However, we can also construct the following counter example in these MUBs:

Counter Example 2 (Case $d = 4$). Let $\{|\Psi_j^\mu\rangle\}_{j=1}^4$ ($\mu = 0,\ldots,4$) be the MUBs given in the above table. Let $\rho = |\varphi\rangle\langle\varphi|$ where

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(1,0,-1,0)^T, \quad (6)$$

and let $\chi = \{|\chi_k\rangle\}_{k=1}^4$ be the orthonormal basis defined by

$$|\chi_1\rangle = \left(\frac{\sqrt{3}i}{2}, \frac{9+3\sqrt{3}i}{32}, \frac{-\sqrt{3}+i}{32}, \frac{3-3\sqrt{3}i}{16}\right)^T,$$

$$|\chi_2\rangle = \left(\frac{\sqrt{3}+i}{4}, \frac{-9\sqrt{3}+9i}{32}, -\frac{\sqrt{3}i}{16}, \frac{3\sqrt{3}+9i}{16}\right)^T,$$

$$|\chi_3\rangle = \left(0, \frac{5-5\sqrt{3}i}{16}, \frac{-3\sqrt{3}-9i}{16}, \frac{3+\sqrt{3}i}{8}\right)^T,$$

$$|\chi_4\rangle = \left(0, \frac{-3+\sqrt{3}i}{8}, -\frac{3i}{4}, \frac{-1-\sqrt{3}i}{4}\right)^T.$$

Then the success probability is given by

$$P_4(\rho,\chi,s_{\max}) = \frac{6493+1065\sqrt{3}}{10240} \simeq 0.8142, \quad (7)$$

which is also strictly greater than Aravind's bound 0.7 for $d = 4$. See also Fig. 1 for numerically generated counter examples.

Since the computations to obtain (5) and (7) are just elementary, we only comment on our choices of the input states (4) and (6). Since the optimal success probability can always be attained by pure input states as mentioned before, we may assume $\rho = |\varphi\rangle\langle\varphi|$ for a unit vector $|\varphi\rangle$ without loss of generality. Now suppose we have $|\langle\Psi_{j_0}^{\mu_0}|\varphi\rangle|^2 = 0$ for some pair (j_0,μ_0). In such a case, if the king chose μ_0 as his measurement basis, then it is already guaranteed (without resort to the physicist's
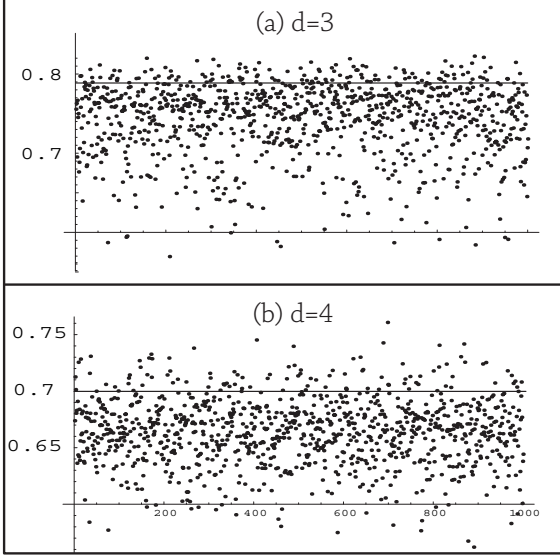
FIG. 1: For (a) $d = 3$ and (b) $d = 4$, the success probability $P_d(\rho, \chi, s_{\max})$ is plotted for 1000 randomly generated PVM measurements. The input states are taken from (4) for $d = 3$ and from (6) for $d = 4$. The solid lines stand for Aravind's bound (3). One finds several counter examples which surpass his bound.

measurement result) that the king's output is absolutely distinct from j_0. This suggests that a better strategy of the physicist is to find an input state which has as many pairs (j, μ) satisfying $|\langle \Psi_j^\mu | \varphi \rangle|^2 = 0$ as possible. In fact, our input states (4) and (6) satisfy the condition $|\langle \Psi_j^\mu | \varphi \rangle|^2 = 0$ at $(j, \mu) = (2, 1), (1, 2), (1, 3), (1, 4)$ and $(j, \mu) = (2, 0), (4, 0), (1, 1), (2, 1), (2, 4), (3, 4)$, respectively.

Now we point out a gap in the proof in [5]. Indeed, it is the first inequality in Claim 1 that cannot be justified, while the second inequality is verified to be true. The crucial error lies in the choice of the decision function s in [5]. Namely, Aravind considered essentially only the decision function given by $s(k, \mu) = f_\mu^{-1}(k)$ where $f_\mu(j) \equiv \operatorname*{argmax}_{k=1,\ldots,d} \left[\langle \Psi_j^\mu | \rho | \Psi_j^\mu \rangle | \langle \Psi_j^\mu | \chi_k \rangle |^2 \right]$ provided that $f_\mu(j)$

is bijective for each μ. In particular, this restriction forces that s must also be bijective for each μ. However this decision function is not optimal in general, and moreover if we choose the input state ρ as discussed above, then the optimal decision function $s_{\max}$ given in (2) is not injective for many μ. Based on this false inference, an argument to "prove" the first inequality is given in [5, Appendix].

We remark that the second inequality in Claim 1 is still valid. Thus Aravind's result can now be stated in the following weaker form:

Theorem 1. *Let* $\{|\Psi_j^\mu\rangle\}_{j=1}^d$ ($\mu = 0, \ldots, d$) *be a set of* $d + 1$ *MUBs. If the input state* ρ *is of the form* $\rho = |\Psi_j^\mu\rangle\langle\Psi_j^\mu|$, *then the success probability* $P_d(\rho, \chi, s)$ *with respect to any basis measurement* χ *and a decision function* s *is bounded from above as*

$$P_d(\rho, \chi, s) \leq \frac{2\sqrt{d} + d - 1}{\sqrt{d}(d+1)}. \qquad (8)$$

Aravind obtained this result by the method of Lagrange multipliers, but here we give an alternate (and possibly simpler but more rigorous) proof for the reader's convenience. We begin with the following lemma:

Lemma 1. *Let* $L \in \mathcal{B}(\mathcal{H})$ *be any bounded operator on a Hilbert space* $\mathcal{H}$ *of the form*

$$L = \sum_{i=1}^m |\phi_i\rangle\langle\phi_i|,$$

where $m \in \mathbb{N}$ *and* $|\phi_i\rangle \in \mathcal{H}$ ($||\phi_i|| = 1$). *Then the operator norm* $||L|| \equiv \sup_{|\psi\rangle \in \mathcal{H}_d \, (||\psi||=1)} ||L|\psi\rangle||$ *has the following upper bound:*

$$||L|| \leq \lim_{n \to \infty} \left(\sum_{i_1,\ldots,i_n=1}^m \prod_{k=1}^{n-1} |\langle\phi_{i_k}|\phi_{i_{k+1}}\rangle| \right)^{\frac{1}{n}}. \qquad (9)$$

Proof. For any $|\psi\rangle \in \mathcal{H}$, we observe

$$||L^n|\psi\rangle||^2 = \sum_{i_1,j_1,\ldots,i_n,j_n=1}^m \langle\psi|\phi_{i_n}\rangle \left(\prod_{k=1}^{n-1} \langle\phi_{i_{k+1}}|\phi_{i_k}\rangle \right) \langle\phi_{i_1}|\phi_{j_1}\rangle \left(\prod_{l=1}^{n-1} \langle\phi_{j_l}|\phi_{j_{l+1}}\rangle \right) \langle\phi_{j_n}|\psi\rangle$$

$$\leq \left(\sum_{i_1,j_1,\ldots,i_n,j_n=1}^m |\langle\phi_{i_1}|\phi_{j_1}\rangle| \left(\prod_{k=1}^{n-1} |\langle\phi_{i_k}|\phi_{i_{k+1}}\rangle| \right) \left(\prod_{l=1}^{n-1} |\langle\phi_{j_l}|\phi_{j_{l+1}}\rangle| \right) \right) ||\psi||^2$$

$$= \left(\sum_{i_1,\ldots,i_{2n}=1}^m \prod_{k=1}^{2n-1} |\langle\phi_{i_k}|\phi_{i_{k+1}}\rangle| \right) ||\psi||^2$$

by the Schwarz inequality. Hence we have

$$||L^n|| \le \sqrt{\sum_{i_1,\dots,i_{2n}=1}^{m} \prod_{k=1}^{2n-1} |\langle \phi_{i_k}|\phi_{i_{k+1}}\rangle|}.$$

By combining this with the Gelfand formula $||L|| = \lim_{n\to\infty} ||L^n||^{\frac{1}{n}}$, we obtain the bound (9). ■

Proof of Theorem 1. We may set $\rho = |\Psi_1^0\rangle\langle\Psi_1^0|$ without loss of generality. Then

$$P_d(\rho,\chi,s_{\max})$$
$$=\frac{1}{d+1}\left[1+\sum_{\mu=1}^{d}\sum_{k=1}^{d}\frac{1}{d}|\langle\Psi_{s_{\max}(k,\mu)}^{\mu}|\chi_k\rangle|^2\right]$$
$$\le\frac{1}{d+1}\left[1+\frac{1}{d}\sum_{k=1}^{d}\left(\sup_{|\psi\rangle}\left[\sum_{\mu=1}^{d}|\langle\Psi_{s_{\max}(k,\mu)}^{\mu}|\psi\rangle|^2\right]\right)\right], \tag{10}$$

where the supremum is over $|\psi\rangle \in \mathcal{H}_d$ such that $||\psi|| = 1$. Let $L \equiv \sum_{\mu=1}^{d} |\Psi_{s(\mu)}^{\mu}\rangle\langle\Psi_{s(\mu)}^{\mu}|$, where s is any real function on $\{1,\dots,d\}$. Since L is positive, it follows that

$$||L|| = \sup_{|\psi\rangle}[\langle\psi|L|\psi\rangle] = \sup_{|\psi\rangle}\left[\sum_{\mu=1}^{d}|\langle\Psi_{s(\mu)}^{\mu}|\psi\rangle|^2\right], \tag{11}$$

where the supremums are over $|\psi\rangle \in \mathcal{H}_d$ with $||\psi|| = 1$. From Lemma 1 and the property [4] of MUBs $|\langle\Psi_i^{\mu}|\Psi_j^{\nu}\rangle|^2 = \delta_{\mu\nu}\delta_{ij} + (1-\delta_{\mu\nu})\frac{1}{d}$, we have

$$||L|| \le \lim_{n\to\infty}\left(\sum_{\mu_1,\dots,\mu_n=1}^{d}\prod_{l=1}^{n-1}|\langle\Psi_{s(\mu_l)}^{\mu_l}|\Psi_{s(\mu_{l+1})}^{\mu_{l+1}}\rangle|\right)^{\frac{1}{n}}$$
$$=\lim_{n\to\infty}\left(\frac{d\sqrt{d}}{\sqrt{d}+d-1}\right)^{\frac{1}{n}}\frac{\sqrt{d}+d-1}{\sqrt{d}}$$
$$=\frac{\sqrt{d}+d-1}{\sqrt{d}}. \tag{12}$$

From (10), (11) and (12), we obtain (8). ■

To summarize, we have constructed some counter examples to Aravind's general bound (3) in [5]. However, we have reconfirmed that it can be justified with restricted input states (Theorem 1). We shall investigate the correct bound which is valid for arbitrary input states in the near future.

[1] L. Vaidman, Y. Aharonov and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987); Y. Aharonov and B.-G. Englert, Z. Naturforsch. A: Phys. Sci. **56a**, 16 (2001); B.-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 1 (2001); P. K. Aravind, Z. Naturforsch. A: Phys. Sci. **58a**, 2212 (2003); T. Durt, e-print quant-ph/0401037.

[2] A. Hayashi, M. Horibe and T. Hashimoto, Phys. Rev. A **71**, 052331 (2005); A. Klappenecker and M. Rötteler, e-print quant-ph/0502138;

[3] G. Kimura, H. Tanaka, and M. Ozawa, Phys. Rev. A, **73**, 050301(R) (2006).

[4] J. Schwinger, Proc. Nat. Acad. Sci. U.S.A. **46**, 570 (1960); I. D. Ivanović, J. Phys. A **14**, 3241 (1981); W. K. Wootters and B. D. Fields, Ann. Physics **191**, 363 (1989); Two orthonormal bases $\{|\Psi_j^{\mu}\rangle\}_{j=1}^{d}$ ($\mu = 0,1$) for a d level system are said to be mutually unbiased if they satisfy the relation $|\langle\Psi_i^{\mu}|\Psi_j^{\nu}\rangle|^2 = \delta_{\mu\nu}\delta_{ij} + (1-\delta_{\mu\nu})\frac{1}{d}$. The maximum number of MUBs is known to be bounded from above by $d+1$, and in fact it is $d+1$ when d is a prime power. It is unknown for all other values of d, even for the smallest case $d=6$.

[5] P. K. Aravind, Z. Naturforsch. **58a**, 682 (2003).

[6] Here we assume d is such that a maximal set of $d+1$ MUBs exists.

[7] If she is allowed to make measurements on the system as well as any ancillary systems which may have been entangled in the preparation phase (Step A), she has a perfect solution proposed recently [1, 2, 3].

[8] O. Schulz, R. Steinhubl, M. Weber, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **90**, 177901 (2003).

[9] Suppose d is an odd prime and let $\{|e_k\rangle\}_{k=1}^{d}$ denote the standard orthonormal basis of $\mathbb{C}^d$. Then, Ivanović [4] constructed $d+1$ MUBs by $|\Psi_j^{\mu}\rangle \equiv \sum_{k=1}^{d} U_{jk}^{(\mu)}|e_k\rangle$, where $U_{jk}^{(\mu)} = \frac{1}{\sqrt{d}}\exp\left[\frac{2\pi i}{d}(\mu+1)(j+k-1)^2\right]$ ($\mu = 0,\dots,d-2$), $U_{jk}^{(d-1)} = \frac{1}{\sqrt{d}}\exp\left[\frac{2\pi i}{d}jk\right]$, and $U_{jk}^{(d)} = \delta_{jk}$.